Notice of Allowability	Application No.	Applicant(s)	
	10/710,350	KRAMER, ANDRE	
	Examiner	Art Unit	
	Samson B. Lemma	2432	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *RCE filed on 04/17/2009*.

2. ☒ The allowed claim(s) is/are *1,4,6-15 and 18-25*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date *03/12 & 04/22/09*.
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

DETAILED ACTION

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on April, 17, 2009 has been entered.

2. Claims 5 and 26-33 are canceled. Furthermore due to the examiner amendment made on 04/22/2009, claims 2-3 and 16-17 are cancelled and are incorporated into the respective independent claims 1 and 15.

3. On March 12, 2009 and subsequently on April 04/22/2009, Applicant's representative Kellan D. Ponikiewicz Registration Number: 59,701 and examiner have conducted a telephone interview. The subject matter of the interview has been attached.

EXAMINER'S AMENDMENT

4. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of

such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Kellan D. Ponikiewicz Registration Number: 59,701 on 04/22/2009.

The application has been amended as follows:

In the claims:

1. (Currently Amended) A method for providing secure access to applications, the method comprising:

(a) receiving a request, from a client system accessed by a user, to execute an application on a server;

(b) determining, by a policy system executing on the server and responsive to receiving the request, a minimal set of computing privileges necessary for the user to use the requested application based in part on an analysis of application requirements; ~~and~~

(c) invoking an execution environment, executing on the server for the user, having the determined set of privileges;

(d) returning an identifier associated with the invoked execution environment to the user; and

(e) connecting, via a remote presentation protocol, the user to the execution environment using the identifier.

2-3. (Cancelled).`

15. (Currently amended) An application server system providing secure access to hosted applications, the system comprising:

a policy based decision system receiving a request from a user to execute an application and determining a minimal set of privileges required by the user to execute the application based in part on an analysis of application requirements; ~~and~~

an account administration service communicating ~~in communication~~ with said policy based decision system, the account administration service invoking an execution environment, for the user, having the determined set of privileges; and

a connection manager communicating with the policy based decision system and with a client via a presentation level protocol, the connection manager transmitting an identification of the user and an identification of the application to the policy based decision system responsive to receiving a request from the user of the client to execute the application.

16-17. (Cancelled).

18. (Currently amended) The system of claim ~~17~~ 15 wherein said presentation-level protocol is selected from the group consisting of RDP, ICA, and X.

Allowable Subject Matter

5. **Claims 1, 4, 6-15 and 18-25** are allowed.

As the result of examiner amendment, Claims 2-3 are canceled and incorporated into independent claim 1 and claims 16-17 are canceled and incorporated into independent claim 15.

6. The following is an examiner's statement of reasons for allowance:

7. Referring to **the independent claims 1 and 15** the art on the record, namely the combination of IBM and **Laksono discloses each and every limitations before the claims were amended.**

For instance, referring to independent claim 1,

IBM, the primary reference on the record, discloses a method for providing secure access to applications *[Page 3, lines 32-34*] (*This is extended by means of a Privilege Control List mechanism, which works in much the same way as the Access Control List mechanism described in the following article)*

the method comprising the steps of:

- **Receiving a request from a user to execute an application**

[Page 4, lines 19-20 and page 4, lines 16-17[On page 4, lines 19-20, see "the command is executed by direct user invocation by shell script or via

system call or subroutine."" and on page 4, lines 16-17, see "any method executing the command");

- **Determining a minimal set of computing privileges necessary for the user to use the requested application** *[Page 3, lines 29-34] (The disclosed mechanism works in conjunction with* ***the least privilege mechanism*** *described in (*), which describes mechanism for associating a set of discrete privileges with a file. This is extended by means of a Privilege Control List mechanism, which works in much the same way as the Access Control List mechanism described in the following article. The submitted specification on paragraph 0005 disclosed the following. "The principle of* ***least privilege ensures that an application runs with the minimal amount of permissions*** *necessary to accomplish its assigned tasks".)*; **and**

- **Invoking an execution environment for the user having the determined set of privileges** *[Page 4, lines 16-18 and page 4, lines 18-21] (On page 4, lines 16-18, the following has been disclosed. "any method of executing the command will 'work' - that is, the* ***invoker will acquire the correct privileges****." Furthermore on page 4, lines 18-21, the following has been disclosed. "this method allows privilege to be acquired whether the command is executed by* ***direct user invocation****, by shell script or via system call or subroutine.")*

Though IBM teaches "the least privilege mechanism" as shown above it does not explicitly disclose "determining a minimal set of

computing privileges necessary for the user to use the requested application"

However, in the same field of endeavor **Laksono on paragraph 0032**, discloses the following.

"The process begins at step 80, where a hand held device of the multimedia system transmits a remote control/monitoring request to a server of the multimedia system" and this meets the limitation recited as "Receiving a request from a user to execute an application" because the hand held device as disclosed on paragraph 0024 could be any kind of device including a laptop which can be operated by the user.

And Laksono on paragraph 0034 discloses the following.

"The process proceeds to step 84 where the server determines remote control and monitoring privileges of the hand held device. The determination of the privileges will be described in greater detail with reference to FIG. 8. The process continues at step 86 where the server **determines whether the hand held device has at least a minimum level of remote control and monitoring privileges."** and this meets the limitation recited as "Determining a minimal set of computing privileges necessary for the user to use the requested application"

And finally Laksono on paragraph 0035 discloses the following.

"If the hand held device has a minimal level of privileges, the process proceeds to step 90, where the server processes the

remote control/monitoring request with respect to at least one of the plurality of clients to produce operational monitoring data." And this meets the limitation recited as "Invoking an execution environment for the user having the determined set of privileges"

Referring to independent claim 15, before the claims were amended, IBM, the primary reference on the record, discloses an application server system providing secure access to hosted applications, *[Page 3, lines 32-34] (On page 3, lines 32-34, the following for instance has been disclosed. This is extended by means of a Privilege Control List mechanism, which works in much the same way as the Access Control List mechanism described in the following article and this meets the limitation recited as "providing secure access to hosted application)* ***the system comprising:***

- **A policy based decision system receiving a request from a user to execute an application** *[On page 3, lines 32-34, the following for instance has been disclosed. This is extended by means of a Privilege Control List mechanism, which works in much the same way as the Access Control List mechanism described in the following article and this meets the limitation of a policy based decision system. Furthermore, on page 3, lines 34-page 4, line 1, the following has been disclosed. A Privilege Control List (PCL) consists of an unordered set of Privilege Control Entries. Each entry consists of a list of typed identifiers and a set of privileges. The list of typed identifiers defines the circumstances under which the privileges will be granted and this also meets the limitation recited as "***A**

policy based decision system") receiving a request from a user to execute an application *(Page 3, lines 32-34, Page 4, lines 19-20 and page 4, lines 16-17][On page 4, lines 19-20, see "the command is executed by direct user invocation by shell script or via system call or subroutine." and on page 4, lines 16-17, see "any method executing the command")*; **and determining a minimal set of privileges required by the user to execute the application** *[Page 3, lines 29-34] (The disclosed mechanism works in conjunction with the least privilege mechanism described in (*), which describes mechanism for associating a set of discrete privileges with a file. This is extended by means of a Privilege Control List mechanism, which works in much the same way as the Access Control List mechanism described in the following article.)*;

- **An account administration service in communication with said policy based decision system, the account administration service invoking an execution environment for the user having the determined set of privileges;** [See page 4, lines 12-23] (On page 4, lines 12-23, the following has been disclosed. *"Since the commands themselves do not enforce policy, the **administrator who controls privilege assignment is free to configure the system roles in whatever manner is appropriate for the local system"**, and this meets "the account administration service". Furthermore the following has been disclosed- "This mechanism is also compatible with existing practice. Because the privilege is associated directly with the program file, any method of executing the command will 'work' - that is, the invoker will*

acquire the correct privileges. Unlike the second mechanism described above, this method allows privilege to be acquired whether the command is executed by direct user invocation, by shell script or via system call or subroutine. - Lastly, this mechanism allows privilege to be granted based on arbitrary combinations of identifiers, thus increasing the flexibility with which the system privilege control policy can be defined" and this meets the limitation "an account administration service in communication with said policy based decision system, the account administration service invoking an execution environment for the user having the determined set of privileges".) and

A connection manager in communication with said policy based decision system *[See again page 4, lines 19-20 and 4, lines 16-17 "the entity/ interface receiving client's request/ execution command meet the limitation of connection manager and this interfaces between the user and the Privilege Control List system/policy based decision system"],* **said connection manager receiving from a client system an RDP request by the user to execute the application** *[Page 4, lines 19-20 and page 4, lines 16-17][On page 4, lines 19-20, see "the command is executed by direct user invocation by shell script or via system call or subroutine."" and on page 4, lines 16-17, see "any method executing the command");***and transmitting to said policy based decision system an identification of said user and an identification of said application.***[See on page 3, lines 32-page 4, line 1 and page 4, lines 16-23] (On page 3, lines 32-page 4, the following has been disclosed. This is extended by means of a*

Privilege Control List mechanism, which works in much the same way as the Access Control List mechanism described in the following article. A Privilege Control List (PCL) consists of an unordered set of Privilege Control Entries. Each entry consists of a list of typed identifiers and a set of privileges. The list of typed identifiers defines the circumstances under which the privileges will be granted. This meets the limitation recited as "policy based decision system based on identification of said user". Furthermore, the following has been stated. "This mechanism is also compatible with existing practice. Because the privilege is associated directly with the program file and this meets the limitation recited as "policy based decision system based on identification of said application", any method of executing the command will 'work' - that is, the invoker will acquire the correct privileges. Unlike the second mechanism described above, this method allows privilege to be acquired whether the command is executed by direct user invocation, by shell script or via system call or subroutine. - Lastly, this mechanism allows privilege to be granted based on arbitrary combinations of identifiers, thus increasing the flexibility with which the system privilege control policy can be defined

Though IBM teaches "the least privilege mechanism" as shown above it does not explicitly disclose "determining a minimal set of computing privileges necessary for the user to use the requested application"

However, in the same field of endeavor **Laksono on paragraph 0032**, discloses the following.

"The process begins at step 80, where a hand held device of the multimedia system transmits a remote control/monitoring request to a server of the multimedia system" and this meets the limitation recited as "Receiving a request from a user to execute an application" because the hand held device as disclosed on paragraph 0024 could be any kind of device including a laptop which can be operated by the user.

And Laksono on paragraph 0034 discloses the following.

"The process proceeds to step 84 where the server determines remote control and monitoring privileges of the hand held device. The determination of the privileges will be described in greater detail with reference to FIG. 8. The process continues at step 86 where the server **determines whether the hand held device has at least a minimum level of remote control and monitoring privileges."** and this meets the limitation recited as "Determining a minimal set of computing privileges necessary for the user to use the requested application"

And finally Laksono on paragraph 0035 discloses the following.

"If the hand held device has a minimal level of privileges, the process proceeds to step 90, where the server processes the remote control/monitoring request with respect to at least one of the plurality of clients to produce operational monitoring data."

And this meets the limitation recited as "Invoking an execution environment for the user having the determined set of privileges"

However independent **claims 1 and 15** are amended. Furthermore as the result of the examiner's amendment dependent claims 2-3 and 16-17 have been canceled and incorporated into the **independent claims 1 and 15 respectively.**

None of the prior art of record taken singularly of in combination teaches or suggests a method for providing secure access to applications and an application server system providing secure access to hosted applications, comprising the amended functional limitation recited in the respective independent claims together with other limitation recited in the claims. For this reason, independent claims **1 and 15** are allowed.

8. The dependent **claims** which are dependent on the above **independent claim 1 and 15** being further limiting to the independent claim, definite and enabled by the specification are also allowed.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submission should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Samson B Lemma whose telephone number is 571-272-3806. The examiner can normally be reached on Monday-Friday (8:00 am---4: 30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, BARRON JR GILBERTO can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Samson B Lemma/

Examiner, Art Unit 2432

/Gilberto Barron Jr./

Supervisory Patent Examiner, Art Unit 2432